バーチャルマシンで実現するコンピュータ・フォレンジックス

Solution of Computer Forensics with Virtual Machines

郡司　啓*　谷川哲司*　支倉健一*
Satoshi Gunji　Tetsuji Tanigawa　Kenichi Hasekura

要　旨

個人情報保護法や不正アクセス禁止法といったコンピュータ・ネットワーク関連法律の整備に伴い，コンピュータの使用状況を正確に記録する「コンピュータ・フォレンジックス」技術が注目されています。この「コンピュータ・フォレンジックス」技術は，情報漏えいやデータ改ざんといったセキュリティインシデントに対し，法的に有効な証拠を残すための手段・手法を指します。

コンピュータ・フォレンジックスによって信頼性の高い証拠を残すことで，セキュリティインシデントの原因調査や，民事訴訟あるいは刑事訴訟への証拠採用が可能となります。しかしこれらの用途に耐える記録を行うには，高度な知識や技術が必要なため，特殊なシステムを構築しない限り実用化は困難と考えられていました。

本稿ではその解決策として，法的証拠能力のある記録を容易に採取可能にする「バーチャルマシンを利用したコンピュータ・フォレンジックス技術」に関して解説します。また，この技術を用いることにより，膨大な時間を要したデータ解析，再現実験を効率的に実現する方法に関しても紹介します。

Computer Forensics is the technique to perpetuate the evidence of security incidents such as the information leakage by the unauthorized access and falsification of data. This technique is useful for the analysis of security incidents. Furthermore, it can provide the evidence for civil lawsuits and criminal trials. However, high level knowledge and skills are needed to collect the evidence for legal purpose. So this technique has been thought difficult to make practical unless integrating the special system.

This paper describes “Computer Forensics with Virtual Machine” that makes collecting legal computer evidence easy. It also introduces effective procedure for data analysis and for reproducing tests, which have taken enormous time.

1．まえがき

近年の情報システムは大規模化・複雑化してきており，それに伴いシステムの開発の際に設計上のミスが入り込む余地が増大しています。そのため，ほぼすべてのシステムにセキュリティホール（本来の手順を踏まずにシステムにアクセスできてしまうような，設計上の欠陥のこと）が存在するといえます。システムにセキュリティホールが存在する場合，不正なアクセスが行われたり，ウイルスやワームに感染したりする可能性があります。

システムが不正なアクセスを受けた場合，もしくはウイルスやワームに感染した場合，情報の漏えいやデータ改ざん，システムの停止といった直接の被害を受けることはもとより，侵入されたシステムを踏み台として利用され，第三者のシステムを攻撃することに利用される恐れもあります（「Internet Security Glossary[1)]」より，これらの事象を総称して「セキュリティインシデント（security incident）」と呼びます）。

今までは，セキュリティインシデントが発生した際に，システムを復旧させることを優先してきました。しかし原因を突き止めないままシステムを復旧すると，再び同じセキュリティホールを利用して不正なアクセスが行われたり，ウイルスやワームに感染したりする可能性があります。またシステムを踏み台にされて第三者のシステムを攻撃することに利用された場合，第三者から損害賠償を請求される可能性もあります。そのため，セキュリティインシデントが発生した際には，セキュリティインシデントの発生原因を分析したり，証拠を保存しておき，訴訟の際に提出したりといった対応が重要になります。

2．コンピュータ・フォレンジックスとは

コンピュータ上で発生したセキュリティインシデントの証拠を残すための一連の作業を総称して，コンピュータ・フォレンジックスと呼びます。

＊ IT基盤システム開発事業部
IT Platform Systems Development Division.

コンピュータの動作やコンピュータが扱うディジタルデータは目に見えないため，「過去にどのようなことが起こったか」を証拠として示すためには，コンピュータ・フォレンジックスが必要となります。

なお，一般にはネットワーク上での通信を長期にわたって取得・保存すること（ネットワーク・フォレンジックス）についてもコンピュータ・フォレンジックスと呼ぶこともありますが，本稿ではサーバ用途のコンピュータ本体における動作の証拠を保存することを対象とします。

2.1 コンピュータ・フォレンジックスの手順

コンピュータ・フォレンジックスの手順は「Guidelines for Evidence Collection and Archiving[2)]」に示されているとおり，揮発性の高い（壊れやすい）データから揮発性の低い（壊れにくい）データの順に保存していきます。典型的な作業手順は，次のようになります。

① 調査対象のコンピュータとは別に，作業用のコンピュータを用意する
② 汚染されていない調査ツールを用意し，調査対象のコンピュータで利用できるようにする
③ 作業用のコンピュータから調査対象のコンピュータにネットワーク経由でリモートログインする
④ 調査ツールにより，ネットワークの状況，プロセス（メモリ・CPU）の状況などの揮発性の高い情報を調査・保存する
⑤ 調査対象のコンピュータを，ネットワークから分離する
⑥ 調査対象のコンピュータの電源を切断してハードディスクを取り出し，作業用のコンピュータにディスクをつなぎ換える
⑦ 作業用のコンピュータで，先ほどのハードディスクのコピーを作成する
⑧ コピー元のハードディスクは証拠として保管する
⑨ コピーしたディスクを対象に，ログなどのディスク上に残された情報を詳細に調査する

2.2 コンピュータ・フォレンジックスの問題点

コンピュータ・フォレンジックスの問題点は，一時対応の時点から高度な技術を持った管理者が対応に当たる必要があることです。フォレンジックスの対象となるコンピュータが今まさに不正侵入されているのか，ウイルスやワームに感染しているのか，被害が他のマシンに及んでいるのかといった状況に応じて，証拠保全をいったん打ち切り，ネットワーク切断などの被害拡大防止に切り替えるなど，臨機応変な対応が求められます。さらに作業を誤ると証拠を破壊してしまうだけでなく，コンピュータ上の大事なデータを消してしまうこともあります。

これらの理由から，コンピュータ・フォレンジックスを実施しようと思った場合には高度な技術が必要となりますが，多くの組織では高度な技術を持った人材の不足やコスト面での理由から，ほとんど実施されませんでした。

3．バーチャルマシンで実現するコンピュータ・フォレンジックス

この問題を解決するために，バーチャルマシンを利用して，コンピュータ・フォレンジックスを実現する方法について述べます。

3.1 バーチャルマシンとは

バーチャルマシンとは，「コンピュータのなかに実現する仮想的なコンピュータ」のことで，実マシンの資源の一部を使用して，あたかもコンピュータのなかにもう一台コンピュータがあるかのように動作します。また実マシンの資源が許す限り，一台の実マシンの上に複数台のバーチャルマシンを動作させることもできます。

バーチャルマシンは，主に「仮想コンピュータタイプ」と「仮想OSタイプ」の2つの種類があります。「仮想コンピュータタイプ」は**図1**のように実マシンのOS上に仮想的なコンピュータを実現します。

仮想コンピュータタイプの場合，バーチャルマシンに導入するOSを自由に選択することができます。このタイプのバーチャルマシンとして代表的なものは，VMWare，Virtual PC，Bochs，QEMUなどがあります。

もう1つの「仮想OSタイプ」は**図2**のように実マシンのOS上に仮想的なOSを実現します。

この場合はバーチャルマシンのOSを選択することはでき

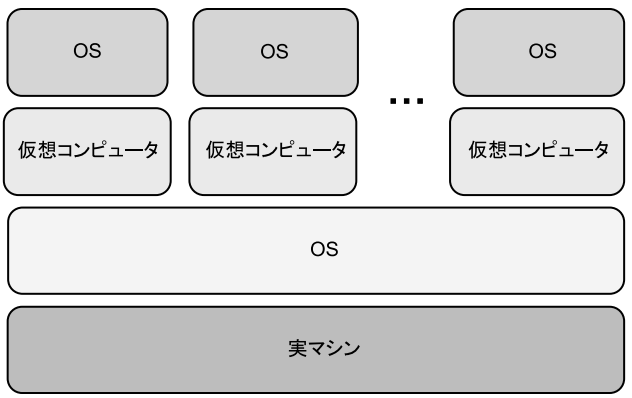

図1 仮想コンピュータタイプのバーチャルマシン
Fig.1 Virtual computer.

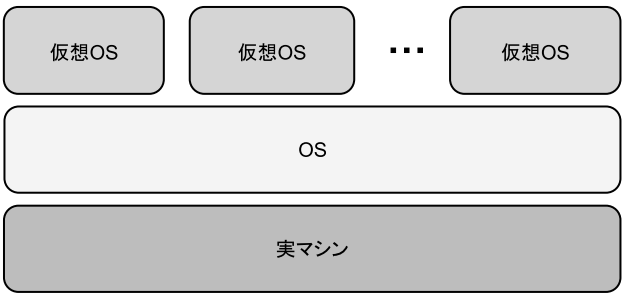

図2 仮想OSタイプのバーチャルマシン
Fig.2 Virtual OS.

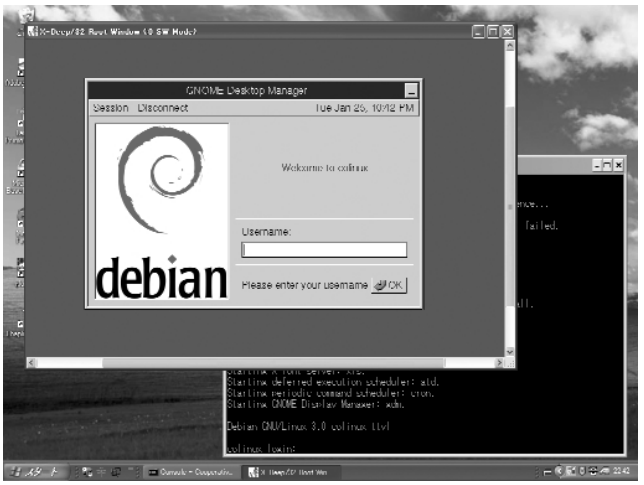

図3　バーチャルマシンの例（coLinux）
Fig.3　Example of Virtual OS (coLinux).

ませんが，「仮想コンピュータタイプ」よりも性能がよくなります。このタイプのバーチャルマシンとして代表的なものは，Linuxマシンの上に仮想Linuxマシンを実現するUser Mode Linux，Windowsマシンの上に仮想Linuxマシンを実現するcoLinux などがあります。**図3**にWindows上でLinuxを動作させるcoLinuxの例を示します。

3.2　バーチャルマシンのコンピュータ・フォレンジックス

多くのバーチャルマシンには，現在の動作状態をそのまま保存する機能があります。動作中のメモリの内容やハードディスクの内容をファイルとして書き出すことができるため，この機能を使えば難しい操作を必要とせずに「ある瞬間のバーチャルマシンの状態」を完全に保存することができます。そのためバーチャルマシンのメモリの内容とハードディスクの内容を，証拠として提出することができます。またこのファイルを利用することでバーチャルマシンを何度でも保存した状態に戻すことができるために，解析を行う際にも証拠の破壊を恐れずに調査できます。

この機能を用いてコンピュータ・フォレンジックスを実現する作業手順を次に示します。

① バーチャルマシンの現在の動作状態を，そのままファイルとして保存する
② 保存したファイルのコピーを作成する
③ 作成したコピーをもとに，バーチャルマシンを立ち上げ直し，ネットワークの状況，プロセス（メモリ・CPU）の状況などの揮発性の高い情報，ログなどのディスク上に残された情報を詳細に調査する

上記の機能を用いてバーチャルマシンの現在の動作状態をそのまま保存するために，バーチャルマシンの動作を止める必要があるものもありますが，バーチャルマシンによっては動作中でも状態を保存する機能があるものもあります。この機能を使えばセキュリティインシデント発生時だけでなく，サーバ用途などの停止させることが困難なマシンに対しても普段から定期的にコンピュータの状態を保存しておくことができるため，復旧や正常な状態との比較を行うことができます。

バーチャルマシンによっては上記のような「現在の動作状態を保存する機能」が実装されていないものもありますが，その場合でもコンピュータ・フォレンジックスの手順を次のとおり簡略化することができます。

① 汚染されていない調査ツールを用意し，調査対象のバーチャルマシンで利用できるようにする
② 実マシンから調査対象のバーチャルマシンに仮想ネットワーク経由でリモートログインする
③ 調査ツールにより，バーチャルマシンのネットワークの状況，プロセス（メモリ・CPU）の状況などの揮発性の高い情報を調査・保存する
④ バーチャルマシンの動作を止めて，バーチャルマシンの仮想ハードディスクファイルをコピーする
⑤ コピー元の仮想ハードディスクファイルは証拠として保管する
⑥ コピーした仮想ハードディスクを対象に，ログなどのディスク上に残された情報を詳細に調査する

4．バーチャルマシンのコンピュータ・フォレンジックスにおける注意点

バーチャルマシンを用いてコンピュータ・フォレンジックスを実現することで，コンピュータ上で起きたことを証拠として残すことが容易になりました。そのため，詳細な調査が必要な場合に，バーチャルマシンの仮想メモリ・仮想ハードディスクファイルを外部の専門家に提供して調査を依頼したり，訴訟の際に証拠として提出したりすることができます。しかし，バーチャルマシンのコンピュータ・フォレンジックスには次のような注意点があります。

まずバーチャルマシンは実マシンと比べてパフォーマンスに劣ります。それ以外にもバーチャルマシンによってはハードディスクやメモリの量が制限されることや，複数のCPUが利用できないなどの機能制限がある場合もあります。そのため取り扱う情報の重要性に応じて，それが本当にコンピュータ・フォレンジックスを必要とするシステムかどうかを決めた上で導入する必要があります。

次にバーチャルマシンを利用することにより証拠を残すことは簡単になりましたが，その証拠を調査分析することについては非常に高度な技術と時間が必要な点は従来と変わりありません。こちらもセキュリティインシデントの重大さとのトレードオフにより，どこまで詳細に調査分析するかを決めることになります。

さらに保存した証拠が本物であることを法的に証明するためには，時刻認証などの別の手段と合わせる必要があります。

5．むすび

従来は「コンピュータセキュリティインシデントを起こ

さない」ことへの対策に注目が集まっていましたが，最近では個人情報保護法や不正アクセス禁止法などへの対応や，架空請求・フィッシング詐欺といったコンピュータ上での事件の多発により，コンピュータ上で起きたことを証拠として残すことに対する重要性が高まりつつあります。

バーチャルマシンによるコンピュータ・フォレンジックスでは証拠を残すことが格段に容易になるため，今まであきらめていたセキュリティインシデントに対する証拠保存を確実に行うことができるようになります。また，こうしてコンピュータ・フォレンジックスの手順の簡略化により，従来は困難であった不正アクセスなどの犯人を発見することの手助けにもなります。

本稿で紹介したバーチャルマシンを活用したコンピュータ・フォレンジックスによって，安心してコンピュータやネットワークを利用できる世の中が実現されることを期待します。

参考文献

1） R. Shirey, “Internet Security Glossary”, FYI 36, RFC 2828, May 2000.

2） D. Brezinski, “Guidelines for Evidence Collection and Archiving”, BCP 55, RFC 3227 Feb 2002.

筆者紹介

Satoshi Gunji

郡司　啓（ぐんじ　さとし） 2000年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター勤務。

Tetsuji Tanigawa

谷川　哲司（たにがわ　てつじ） 1985年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターコンサルティングマネージャー 兼 ユビキタスソフトウェア事業部コンサルティングマネージャー。

Kenichi Hasekura

支倉　健一（はせくら　けんいち） 1991年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターコンサルティングマネージャー。